Noname manuscript No.
(will be inserted by the editor)

Tweaking a Block Cipher: Multi-user Beyond-Birthday-Bound Security in the Standard Model*

Benoît Cogliati

Received: date / Accepted: date

Abstract In this paper, we present a generic construction to create a secure tweakable block cipher from a secure block cipher. Our construction is very natural, requiring four calls to the underlying block cipher for each call of the tweakable block cipher. Moreover, it is provably secure *in the standard model* while keeping the security degradation minimal in the multi-user setting. In more details, if the underlying blockcipher E uses $n-$bit blocks and $2n-$bit keys, then our construction is proven secure against multi-user adversaries using up to roughly 2^n time and queries as long as E is a secure block cipher.

Keywords tweakable block cipher · prp-to-prf conversion · multi-user security · XORP construction · standard model

Mathematics Subject Classification (2000) 94A60

* This is a post-peer-review, pre-copyedit version of an article published in Designs, Codes and Cryptography. The final authenticated version is available online at: http://dx.doi.org/10.1007/s10623-018-0471-8

University of Luxembourg, Luxembourg
E-mail: benoitcogliati@hotmail.fr

1 Introduction

Tweakable Block Ciphers. Tweakable block ciphers generalize the notion of block cipher by allowing an (eventually public) additional parameter $t \in \mathcal{T}$ which is called a tweak. This new parameter has been introduced to bring an inherent variability to the encryption, like an IV or a nonce for a mode of operation. The relevant definitions and security notions have first been formally defined in a paper by Liskov, Rivest and Wagner [27]. Informally, a tweakable block cipher should be indistinguishable from a random tweakable permutation, i.e. a family of permutations indexed by $\mathcal{T}$. This primitive has since then been shown to be useful for several applications like length preserving modes of operations [18,19], online encryption [45,1], authenticated encryption [27,44, 43] and full disk encryption. A few natively tweakable block ciphers already exist, like the Hasty Pudding Cipher [47], Mercy [12], or Threefish (which is used in the Skein [15] hash function). Jean *et al.* [22] also defined the TWEAKEY framework, which can be used to create tweakable block ciphers from scratch.

Generic Constructions from Block Ciphers. Tweakable block ciphers can be built generically from standard block ciphers, and this is the approach we follow in this work. Several such constructions can already be found in the literature. These constructions often rely on an $\varepsilon-\mathsf{AXU}$ family of functions, i.e. a family of keyed functions satisfying the following condition:

$$\forall t \in \mathcal{T}, \forall t' \in \mathcal{T} \setminus \{t\}, \forall y \in \{0,1\}^n, \Pr\left[h \leftarrow_{\$} \mathcal{H} : h(t) \oplus h(t') = y\right] \leq \varepsilon.$$

Let us fix a block cipher E with key space $\mathcal{K}$ and message space $\{0,1\}^n$ and a $\varepsilon-\mathsf{AXU}$ family of hash functions $\mathcal{H}$ from a set $\mathcal{T}$ to $\{0,1\}^n$. In their seminal paper, Liskov *et al.* [27] already proposed two different generic constructions and got a proof of security up to the birthday bound. These constructions are defined as follows. For each $t \in \mathcal{T}$, $k \in \{0,1\}^n$, $m \in \{0,1\}^n$ and $h \in \mathcal{H}$, one has

$$\begin{aligned} \mathrm{LRW}^1_k(t,m) =& E_k(t \oplus E_k(m)), \\ \mathrm{LRW}^2_{h,k}(t,m) =& h(t) \oplus E_k(m \oplus h(t)), \end{aligned}$$

These constructions are very simple and thus very useful. However, their security is limited to the birthday bound, which can make them too weak for some applications. There exists numerous other black-box strategies to build a tweakable block ciphers. One can cite e.g. XEX [43]and its variants [32,7] which are linked to Liskov *et al.*'s first construction and suffer from the same limitation to the birthday bound.

More recently, a few beyond-the-birthday-bound secure constructions have been published. For example, one can remark that the LRW^2 construction can be iterated with independent keys, thus increasing the security of the construction beyond the birthday bound and making it asymptotically grow towards optimal security as the number of rounds grows [25,24,42]. This construction is however quite inefficient if the security requirements are high.

There also exist other constructions which are both beyond the birthday bound secure and do not require being iterated. The first one is Minematsu's construction [33], denoted Min, or Mennink's constructions [29], denoted $\tilde{F}[1]$ and $\tilde{F}[2]$

$$
\begin{aligned}
&\mathrm{Min}_k(t,m) = E(E(k, \underbrace{t}_{\theta \text{ bits}} || \underbrace{0\cdots0}_{n-\theta \text{ bits}}), m) && \text{for every } (t,k,m) \in \{0,1\}^\theta \times (\{0,1\}^n)^2 \\
:& \\
&\tilde{F}[1]_k(t,m) = E_{k\oplus t}(m \oplus k \otimes t) \oplus k \otimes t && \text{for every } (k,t,m) \in (\{0,1\}^n)^3 \\
&\tilde{F}[2]_k(t,m) = E_{k\oplus t}(m \oplus E_k(t)) \oplus E_k(t) && \text{for every } (k,t,m) \in (\{0,1\}^n)^3
\end{aligned}
$$

where $\otimes$ denotes the product on the finite field with 2^n elements, for an arbitrary fixed irreducible polynomial. A necessary condition for the security of Minematsu's construction is that the number of adversarial queries has to be small in front of $2^{n-\theta}$, which means that the security of the construction grows as the size of the tweak space shrinks. Mennink's constructions are secure as long as the number of queries is small in front of $2^{2n/3}$, respectively 2^n. The only drawback of these two constructions is that the security proof only holds in the ideal cipher model, as opposed to the other constructions which are studied in the standard model[1]. In [49], the constructions $\tilde{F}[1]$ and $\tilde{F}[2]$ have been completed by 32 related constructions that also achive 2^n provable security in the ideal cipher model.

Multi-User security. Unfortunately, none of the existing constructions offering beyond the birthday bound security in the standard model can really be considered practical. However, all these constructions were studied in the single user setting. Yet, block ciphers are typically widely deployed and are used with a lot of different keys. Multi-user security thus appears as a very natural security notion. This notion was first introduced and formalized by Bellare, Boldyreva and Micali [2] in the context of public-key encryption. Recently, several works by Mouha and Luykx [35], Tessaro [48], Hoang and Tessaro [20] and Luykx, Mennink and Paterson [28] study the multi-user security for block-cipher designs. A natural question is to investigate whether it is possible to build a secure tweakable block cipher from a multi-user secure block cipher, by using a different key for the underlying block cipher for each different tweak.

Our contribution. In this paper, we propose a new simple method to construct a tweakable block cipher from a block cipher. We also prove its security in the standard model and the multi-user setting as long as the block cipher is secure and the number of adversarial queries is small in front of 2^n, where n is the size of the block. We now describe our construction. Let $n > 1$ be an integer. Let E be a block cipher with key space $\{0,1\}^{2n}$ and message space $\{0,1\}^n$. We define the tweakable block cipher E' with key space $\{0,1\}^{2n}$, tweak space $\{0,1\}^{n-2}$ and message space $\{0,1\}^n$ as follows. For every $(k,t,m) \in \{0,1\}^{2n} \times \{0,1\}^{n-2} \times \{0,1\}^n$, one has

$$E'(k,t,m) = E\left(E(k,t||0) \oplus E(k,t||1) || E(k,t||0) \oplus E(k,t||2), m\right),$$

[1] It is still possible to study Mennink's constructions in the standard model, however the result will have to use the security of the underlying block cipher against some family of related key attacks.

where $||$ denotes the concatenation operation and we use 2-bit encoding for $t||i$, for $i = 0, 1, 2$. This construction requires four calls to the underlying block cipher, while offering a tweak space only four times smaller than the message space and enjoying a very interesting security bound. However, we require tweak-dependent re-keying, which may prove costly in a real world implementation.

Our security proof relies on two results. First we show how to build a secure tweakable block cipher from a secure block cipher and a pseudo-random function. Then we extend to the multi-user setting a result from [21] showing that, when P is a uniformly random permutation, then $x \mapsto \mathsf{XORP}^w_P(x) = \big|\big|_{i=1}^{w} P(x||0) \oplus P(x||i)$ is indistinguishable from a uniformly random function. As usual, this last security proof relies on Patarin's H coefficients technique [38].

A NOTE ON THE χ^2 METHOD. In [13], the authors formalized a new proof technique named the χ^2 method. They used it to provide very simple security proofs for the (full) indistinguishability of the XORP^2 construction and of the XOR of two permutations. Unfortunately, Bhattacharya and Nandi identified a flaw in the proofs [5]. In a subsequent article [4], Bhattacharya and Nandi manage to prove the (full) indifferentiability of the XOR of two (or more) independent permutations via the χ^2 method. The generalization of this proof to the XORP^w construction for $w \geq 2$ is still an interesting and challenging open problem.

RELATED WORK. In [36], the author independently defines a construction that is fairly similar to our own. They combine the XORP construction for tweak and key deriving function with the LRW construction to get a tweakable block cipher. However, they study it with AE in mind, in the single-user setting. More precisely, they consider the tweak as a nonce and a counter, the nonce being fed to the XORP construction and the counter to the XOR universal hash function. This is made to prevent frequent rekeying of the block cipher. With this approach, the primitive that is being studied is more a tweakable (or rather nonce-based) mode of operation for a block cipher rather than a generic BC-to-TBC conversion technique. On the contrary, we focus on the conversion aspect of the construction and more specifically on the multi-user security rather than the single-user security.

In [26], the authors prove a result which is also similar to our Theorem 2. There are still several differences: the security of the tweakable block cipher is considered in the single-user setting and the constructions are allowed to depend on some idealized primitives. They also use this result in a different context and apply it to iterated constructions (the Even-Mansour [14] and Tweakable Even-Mansour [11] constructions and the iterated LRW [27] construction).

In [31], Mennink presents an impossibility result regarding the construction of an optimally secure tweakable block cipher from a block cipher in the standard model using standard proof techniques. This is deeply related to our results and we include a discussion on the the topic of optimal security in section 3.2.

More related work. Another way of building a secure tweakable block cipher is to create it "from scratch", i.e. using a lower level idealized primitive. The first provably secure high level structures allowing the construction of natively tweakable block ciphers from lower-level primitives have been studied by Goldenberg *et al.* [16] who considered the inclusion of a tweak in a Feistel network. This work has then been extended to generalized Feistel networks by Mitsuda and Iwata [34]. A similar study has been undertaken for the class of key-alternating ciphers in a long series of articles by Cogliati and Seurin [11,10], Cogliati, Lampe and Seurin [9], Granger *et al.* [17], Kurosawa [23], Mennink [30] and Sasaki *et al.* [46].

2 Preliminaries

General notations. The set of binary strings of length n is denoted $\{0,1\}^n$. For every integer n, we will sometimes denote $[n] = \{1,\ldots,n\}$. Given a non-empty set $\mathcal{X}$, we denote $x \leftarrow_{\$} \mathcal{X}$ the uniformly random draw of x in the set $\mathcal{X}$. For any positive integer a, let $I_n^a = (\{0,1\}^n)^a$ and let J_n^a be the set of tuples $(x_1,\ldots,x_a) \in I_n^a$ such that the x_is are pairwise distinct. For any integers $1 \leq b \leq a$, we will write $(a)_b = a(a-1)\cdots(a-b+1)$ and $(a)_0 = 1$ by convention. The set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted $\mathsf{Func}(\mathcal{X},\mathcal{Y})$, and the set of all permutations of $\mathcal{X}$ is denoted $\mathsf{Perm}(\mathcal{X})$. The set of all permutations of $\{0,1\}^n$ is simply denoted $\mathsf{Perm}(n)$. A family of permutation of a set $\mathcal{X}$ indexed by a set $\mathcal{Y}$ is denoted $\mathsf{Perm}(\mathcal{Y},\mathcal{X})$. We will also often see a family $\widetilde{P} \in \mathsf{Perm}(\mathcal{X},\mathcal{Y})$ as a function $\widetilde{P} : \mathcal{X}\times\mathcal{Y} \to \mathcal{Y}$ such that, for each $x \in \mathcal{X}$, $\widetilde{P}(x,\cdot) = \widetilde{P}_x$ is a permutation. When the set $\mathcal{X}$ is of the type $\{0,1\}^n$ for an integer n, we will simply write $\mathsf{Perm}(\mathcal{Y},n)$ instead of $\mathsf{Perm}(\mathcal{Y},\{0,1\}^n)$. A multi-user permutation with u users and domain $\mathcal{X}$ is a family of permutations indexed by the set $[u]$. A tweakable permutation with tweak space $\mathcal{T}$ is a family of permutations indexed by the set $\mathcal{T}$.

Security notions. We consider the security of our constructions in the standard, non-idealized model, in the multi-user setting. Let $\mathcal{K},\mathcal{M}$ be two non-empty sets and let u be the number of users. The set $\mathcal{K}$ will be referred to as the set of users and $\mathcal{M}$ the set of messages. Each user will be assigned a uniformly random key that will be kept secret from the adversary. This assignment will be modeled as the uniformly random draw of a function $f \in \mathsf{Func}([u],\mathcal{K})$.

Let q,t be two positive integers and let $E : \mathcal{K}\times\mathcal{M} \to \mathcal{M}$ be a block cipher. We write $E_k(x)$ for $E(k,x)$. A $(u,q,t)-$adversary D against the multi-user strong PRP security (shortened to $\pm$mPRP) of E is an algorithm with oracle access to a multi-user permutation $P \in \mathsf{Perm}([u],\mathcal{M})$, making a total of at most q adaptive and bidirectional oracle queries to at most u distinct users, running in time at most t and outputting a single bit. The advantage of D in

breaking the ±mPRP-security of E is defined as

$$\mathbf{Adv}_{E}^{\pm\mathrm{mPRP}}(\mathsf{D}) = \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}) \,:\, \mathsf{D}^{E(f(\cdot),\cdot)} = 1\right] - \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}([u],\mathcal{M}) \,:\, D^{\widetilde{P}} = 1\right] \Big|.$$

Let $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$ be a tweakable block cipher. We write $\widetilde{E}_k(t,x)$ for $\widetilde{E}(k,t,x)$. A (u,q,t)−adversary D against the multi-user strong TPRP security (shortened to $\pm\mathrm{m}\widetilde{\mathrm{PRP}}$) of $\widetilde{E}$ is an algorithm with oracle access to a multi-user tweakable permutation $P \in \mathsf{Perm}([u] \times \mathcal{T}, \mathcal{M})$, making a total of at most q adaptive and bidirectional oracle queries to at most u users, running in time at most t and outputting a single bit. The advantage of D in breaking the $\pm\mathrm{m}\widetilde{\mathrm{PRP}}$-security of $\widetilde{E}$ is defined as

$$\mathbf{Adv}_{\widetilde{E}}^{\pm\mathrm{m}\widetilde{\mathrm{PRP}}}(\mathsf{D}) = \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}) \,:\, \mathsf{D}^{\widetilde{E}(f(\cdot),\cdot,\cdot)} = 1\right] - \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}([u] \times \mathcal{T},\mathcal{M}) \,:\, D^{\widetilde{P}} = 1\right] \Big|.$$

Let $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ be a keyed function. We write $F_k(x)$ for $F(k,x)$. A (u,q,t)−adversary D against the multi-user PRF security (shortened to mPRF) of F is an algorithm with oracle access to a function $F \in \mathsf{Func}([u] \times \mathcal{X}, \mathcal{Y})$ making a total of at most q adaptive oracle queries to at most u users, running in time at most t and outputting a single bit. The advantage of D in breaking the mPRF security of F is defined as

$$\mathbf{Adv}_{F}^{\mathrm{mPRF}}(\mathsf{D}) = \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}) \,:\, \mathsf{D}^{F(f(\cdot),\cdot)} = 1\right] - \Pr\left[R \leftarrow_{\$} \mathsf{Func}([u] \times \mathcal{X},\mathcal{Y}) \,:\, D^{R} = 1\right] \Big|.$$

3 Rationale behind the constructions

3.1 Description of the Constructions and Summary of the Results

Let $\mathcal{K}_E, \mathcal{K}_F, \mathcal{M}_F$ be non-empty sets and let $n > 1$ be an integer. Let $F : \mathcal{K}_F \times \mathcal{M}_F \to \mathcal{K}_E$ be a PRF and let $E : \mathcal{K}_E \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. As in [33], we define the tweakable block cipher $\mathsf{TKS}[E,F]$ with key space $\mathcal{K}_F$, tweak space $\mathcal{M}_F$ and message space $\mathcal{M}_E$ as follows:

$$\forall (k,t,m) \in \mathcal{K}_F \times \mathcal{M}_F \times \{0,1\}^n,\ \mathsf{TKS}[E,F]_k(t,m) = E_{F_k(t)}(m).$$

In section 4, we prove in Theorem 2 that this construction enjoys a security reduction in the multi-user setting to the mPRF security of F and the $\pm$mPRP security of E. Namely, we prove that, for any positive integers q, t, any number of users u, and any $(u, q, t)-$adversary D against the $\pm\widetilde{\mathrm{mPRP}}$ security of $\mathsf{TKS}[E, F]$, there exist a $(u, \tau, t')-$adversary D' against the mPRF$-$security of F, where $\tau = \min(q, u \cdot |\mathcal{M}_F|)$, and a (τ, q, t'') adversary D'' against the $\pm$mPRP security of E such that

$$\mathbf{Adv}^{\pm\widetilde{\mathrm{mPRP}}}_{\mathsf{TKS}[E,F]}(\mathsf{D}) \leq \mathbf{Adv}^{\mathrm{mPRF}}_{F}(\mathsf{D}') + \mathbf{Adv}^{\pm\mathrm{mPRP}}_{E}(\mathsf{D}''),$$

where $t' = O(t + q \cdot t_E)$, $t'' = t + O(q)$, and t_E denotes an upper bound on the time needed to compute E and E^{-1} on any input.

With this result in mind, it seems natural to use PRP-to-PRF conversion methods in order to replace the PRF F by a construction based on the block cipher E. Minematsu's construction can be seen as a particular case of this family of constructions, using a block cipher as a PRF. What makes Minematsu's construction beyond the birthday bound secure in the single user setting is the fact that the tweak size is kept small enough[2]. In this case, in the security reduction, the number of queries made to the PRF correspond to the number of different tweaks used is certainly smaller than $u \cdot |\mathcal{M}_F|$, thus introducing a term $\min(q, u \cdot |\mathcal{M}_F|)^2/|\mathcal{M}_E|$ in the security bound. In the multi-user setting, shrinking the tweak space will not be very helpful to prove beyond-birthday-bound security in this new setting, as long as the number of users is supposed to be high. Indeed, it is desirable to have a tweak space as large as possible. In order to keep an efficient construction while being able to prove security beyond the birthday bound, we will have to use a better PRF than a block cipher. Namely, we will use the XORP^w_E construction which is defined as follows [21]:

$$\forall (k, m) \in \mathcal{K}_E \times \{0,1\}^{n-\lceil \log_2(w+1) \rceil}, \mathsf{XORP}^w_E(k, m) = ||_{i=1}^{w} E_k(m||0) \oplus E_k(m||i),$$

where $||$ denotes the concatenation operation. We will also consider the truncated XORP construction which we will denote $\mathsf{XORP}^{w,s}_E := \mathrm{Trunc}_s \circ \mathsf{XORP}^w_E$, where Trunc_s denotes the truncation operation where we drop the last $t-s$ bits of a t-bit string, where $t \geq s$. In section 5, we prove that the $\mathsf{XORP}^{w,s}_E$ construction enjoys the same security bound in the multi-user setting than the XORP^w_E in the single-user setting. Namely, for any number u of users, any positive integers q, t, s such that $q \leq \frac{2^n}{w^2(w+1)}$, $s \leq wn$ and any $(u, q, t)-$adversary D against the mPRF security of $\mathsf{XORP}^{w,s}_E$, there exists a $(u, (w+1)q, t')-$adversary against the mPRP security of E such that

$$\mathbf{Adv}^{\mathrm{mPRF}}_{\mathsf{XORP}^w_E}(\mathsf{D}) \leq \mathbf{Adv}^{\mathrm{mPRP}}_{E}(\mathsf{D}') + \frac{w^2 q}{2^n},$$

[2] This also holds in the multi-user setting as long as the set of users is small enough.

where $t' = O(t + q \cdot t_{\mathrm{XORP}_{w,s}})$, and $t_{\mathrm{XORP}_{w,s}}$ is an upper bound on the time needed evaluate the $\mathsf{XORP}_{\cdot}^{w,s}$ construction.

If we combine these two results, we get the following theorem which is the main contribution of this work.

Theorem 1 *Let u be the number of users. Let k, n, q, t be positive integers such that $n > 1$ and $w^2(w+1)q \leq 2^n/67$ where $w := \lceil k/n \rceil$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let D be a $(u, q, t)-$adversary against the $\pm\widetilde{\mathrm{mPRP}}$ security of $\mathsf{TKS}[E, \mathsf{XORP}_E^{w,k}]$. Then there exist a $(u, (w+1)\tau, t')$-adversary against the* mPRP *security of E and a $(\tau, q, t'')-$adversary against the* $\pm$mPRP *security of E such that*

$$\mathbf{Adv}^{\pm\widetilde{\mathrm{mPRP}}}_{\mathsf{TKS}[E,\mathsf{XORP}_E^{w,k}]}(\mathsf{D}) \leq \mathbf{Adv}^{\mathrm{mPRP}}_{E}(\mathsf{D}') + \mathbf{Adv}^{\pm\mathrm{mPRP}}_{E}(\mathsf{D}'') + \frac{w^2 q}{2^n},$$

where $\tau = \min(q, u \cdot 2^{n-1-\lfloor \log_2(w) \rfloor})$, $t' = O(t + q \cdot (t_{XORP_{w,k}} + t_E))$, $t'' = t + O(q)$, t_E denotes an upper bound on the time needed to compute E and E^{-1} on any input and $t_{XORP_{w,k}}$ is an upper bound on the time needed evaluate the $\mathsf{XORP}_{\cdot}^{w,k}$ construction.

Remark 1 Under the assumption that E is secure as long as $u, q, t \ll 2^n$, Theorem 1 implies that our construction results in a tweakable block cipher that is also secure under the same constraints in the standard model, while it still offers interesting performances. Namely, a change of tweak requires $w + 1$ encryptions and a rekeying of E, while encrypting/decrypting a block (without changing the tweak) simply costs one call to E.

Remark 2 While it would seem natural to choose a block cipher using a n-bit key, where n is the size of the block, this would only lead to birthday bound security. Consider the following multi-user adversary D against such a block cipher, due to Biham [6]:

- D chooses an arbitrary fixed message, encrypts it for about $2^{n/2}$ distinct users using its encryption oracle;
- D chooses about $2^{n/2}$ keys and computes the encryption of this message under the chosen keys;
- for each collision between the two sets of ciphertexts, D tests if the guessed key is correct by encrypting a second message; if it is, D assumes it has found the key of the corresponding user.

Such an adversary can recover at least one key with a high probability, while only requiring about $2^{n/2}$ time and queries. Thus, for our scheme to be truly secure up to 2^n time and queries, it is necessary to chose a block cipher whose key size is at least twice the block length.

3.2 A note on Optimality

Let u, k, n be three integers and let $E, : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher.

In [31], Mennink defines optimal security as follows: E will be said optimally secure if, for every single user adversary D allowed q queries and a computation time t, one has

$$\mathbf{Adv}_{E}^{\pm\mathrm{mPRP}}(\mathsf{D}) \leq \frac{\mathrm{const}_E \cdot \max(q,t)}{\min(2^k, 2^n)},$$

where const_E is a small constant depending on E. Optimal security for tweakable block ciphers is defined similarly. He investigates the possibility of building a tweak-rekeyable cipher (i.e. a tweakable block cipher based on a block cipher, where the value of the tweak influences the value of the key used for the underlying block cipher) and proving its security in the standard model by using generic standard-to-ideal transformations. He proves that, assuming that the best possible security for a non-tweak-rekeyable tweakable block cipher based on a block cipher is $2^{\sigma n/(\sigma+1)}$, then it is impossible to achieve optimal security with such a proof technique. This result stems from the fact that either the tweak has little influence over the value of the key used by the underlying block cipher, in which case the construction shares the same bound as non-tweak-rekeyable constructions, or the tweak has a great influence. In the latter case, the underlying block cipher will be used with a lot of different keys, and thus be vulnerable to a (related-key) key recovery attack. In our work, we discuss the merit of shifting from the single-user scenario to the multi-user scenario.

In order to better see the benefits of the multi-user setting, we are going to choose a slightly different definition of optimal security by generalizing to the multi-user setting the notion from [3, Section 3.6]. We are going to say that the block cipher E is optimally secure if, for any adversary D allowed q queries to at most u users and a computation time t, one has

$$\mathbf{Adv}_{E}^{\pm\mathrm{mPRP}}(\mathsf{D}) \leq \frac{c_E u t}{2^k} + \frac{c'_E q}{2^n},$$

where c_E and c'_E are small constants. Optimally secure tweakable block ciphers using the same key space and message space as E would be defined by the exact same condition[3].

Using Theorem 1, and assuming optimal security for E, for any adversary D allowed q queries to at most u users and a computation time t, we have

$$\mathbf{Adv}^{\pm\mathrm{m}\widetilde{\mathrm{PRP}}}_{\mathsf{TKS}[E,\mathsf{XORP}^{w,k}_{E}]}(\mathsf{D}) \leq \frac{c_E u t' + c_E \tau t''}{2^k} + \frac{\left(w^2 + c'_E(w+2)\right) q}{2^n},$$

where $\tau = \min(q, u \cdot 2^{n-1-\lfloor \log_2(w) \rfloor})$, $t' = O(t + q \cdot (t_{\mathrm{XORP}_{w,k}} + t_E))$, $t'' = t + O(q)$, t_E denotes an upper bound on the time needed to compute E and E^{-1} on any input and $t_{\mathrm{XORP}_{w,k}}$ is an upper bound on the time needed evaluate the $\mathsf{XORP}^{w,k}_{\cdot}$ construction. Hence one has

$$\mathbf{Adv}^{\pm\mathrm{m}\widetilde{\mathrm{PRP}}}_{\mathsf{TKS}[E,\mathsf{XORP}^{w,k}_{E}]}(\mathsf{D}) \leq \frac{\tilde{c}_E u t + \tilde{c}'_E u q + c_E q t + \tilde{c}''_E q^2}{2^k} + \frac{\left(w^2 + c'_E(w+2)\right) q}{2^n},$$

[3] Note that the first term involves the number u of users in order to capture Biham's multi-user key search attack.

where $\tilde{c}_E$, $\tilde{c}'_E$ and $\tilde{c}''_E$ are small constants. Several remarks can then be done:

- in the single-user setting ($u = 1$), our construction would achieve the same security bound as Minematsu's construction (namely birthday bound security with respect to the key size if we take the largest available tweak space, or beyond the birthday bound security if we restrict the tweak space);
- in the case where $k \geq 2n$,
  - our construction achieves n bits of security;
  - in the multi-user setting, and assuming that the adversary can access as many users as it desires ($u = q \leq 2^n$), our construction actually achieves optimal security (however this is not the case if $u \ll q$).

This does not contradict the result from [31], and the issues raised in this article are relevant and underline interesting questions:

- is the "real" security of a system closer to idealized-model security or standard-model security?
- can generic standard-to-ideal reductions be avoided?

In this article, we stay in the standard model and show that, even if the security loss from the rekeying of the underlying block cipher depending on the tweak is unavoidable due to the looseness of Theorem 2, in the multi-user setting it can be somewhat mitigated (depending on the power given to the adversary). Indeed, a similar security loss becomes mandatory and has to be taken into account in the notion of optimal security[4].

4 The Security of the TKS Construction

One has the following result. It can be seen as the multi-user version of Theorem 3 from [33].

Theorem 2 *Let u be the number of users. Let $\mathcal{K}_E, \mathcal{K}_F, \mathcal{M}_E, \mathcal{M}_F$ be non-empty sets and let q, t be positive integers. Let $F : \mathcal{K}_F \times \mathcal{M}_F \to \mathcal{K}_E$ be a PRF and let $E : \mathcal{K}_E \times \mathcal{M}_E \to \mathcal{M}_E$ be a block cipher. Let D be a $(u, q, t)-$adversary against the $\pm\widetilde{\text{mPRP}}$ security of $\mathsf{TKS}[E, F]$. Then there exist a $(u, \tau, t')-$adversary D' against the* mPRF *security of F and a (τ, q, t'') adversary D'' against the* $\pm$mPRP *security of E such that*

$$\mathbf{Adv}^{\pm\widetilde{\text{mPRP}}}_{\mathsf{TKS}[E,F]}(\mathsf{D}) \leq \mathbf{Adv}^{\text{mPRF}}_{F}(\mathsf{D}') + \mathbf{Adv}^{\pm\text{mPRP}}_{E}(\mathsf{D}''),$$

where $\tau = \min(q, u \cdot |\mathcal{M}_F|)$, $t' = O(t + q \cdot t_E)$, $t'' = t + O(q)$, and t_E denotes an upper bound on the time needed to compute E and E^{-1} on any input.

Remark 3 Note that, if $u = 1$, then we can recover Theorem 3 from [33] by applying the standard multi-user to single-user security reduction.

[4] If we consider the multi-user setting, the multi-user key search attack [6] mitigates the impact of the related-key attack from [31] as the number of distinct users grows to the number of adversarial queries.

Proof of Theorem 2. Let D be a $(u,q,t)-$adversary against the $\pm\mathrm{m}\widetilde{\mathrm{PRP}}$ security of $\mathsf{TKS}[E,F]$. Let us denote F^* the perfect PRF whose key space is simply $\mathcal{K}_{F^*} = \mathsf{Func}(\mathcal{M}_F, \mathcal{K}_E)$, such that

$$\forall (k,x) \in \mathcal{K}_{F^*} \times \mathcal{M}_F,\ F^*_k(x) = k(x).$$

Then, by definition, one has

$$\begin{aligned}
\mathbf{Adv}^{\pm\mathrm{m}\widetilde{\mathrm{PRP}}}_{\mathsf{TKS}[E,F]}(\mathsf{D}) = &\Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_F) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F]_{f(\cdot)}} = 1\right] \\
&\qquad - \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}([u]\times\mathcal{M}_F, \mathcal{M}_E) \,:\, \mathsf{D}^{\widetilde{P}} = 1\right]\Big| \\
\leq &\Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_F) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F]_{f(\cdot)}} = 1\right] \\
&\qquad - \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_{F^*}) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F^*]_{f(\cdot)}} = 1\right]\Big| \\
&+ \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_{F^*}) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F^*]_{f(\cdot)}} = 1\right] \\
&\qquad - \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}([u]\times\mathcal{M}_F, \mathcal{M}_E) \,:\, \mathsf{D}^{\widetilde{P}} = 1\right]\Big|.
\end{aligned}$$

Then it is easy to see that there exists a $(u,\tau,t')-$adversary D' against the mPRF$-$security of F such that

$$\begin{aligned}
&\Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_F) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F]_{f(\cdot)}} = 1\right] \\
&\qquad - \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_{F^*}) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F^*]_{f(\cdot)}} = 1\right]\Big| \leq \mathbf{Adv}^{\mathrm{mPRF}}_F(\mathsf{D}'), \quad (1)
\end{aligned}$$

where $t' = O(t + q \cdot t_E)$ and $\tau = \min(q, u \cdot |\mathcal{M}_F|)$. Indeed, D has to distinguish between the multi-user tweakable permutations $E_{F_{f(\cdot)}(\cdot)}(\cdot)$ and $E_{F^*_{f(\cdot)}(\cdot)}(\cdot)$. Since, when $f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_{F^*})$, $F^*_{f(\cdot)}$ is simply a uniformly random function from $\mathsf{Func}([u]\times\mathcal{M}_F,\mathcal{K}_E)$, an equivalent description would be to say that D has to distinguish between $E_{F_{f(\cdot)}(\cdot)}(\cdot)$, where $f \leftarrow_{\$} \mathsf{Func}([u],\mathcal{K}_F)$, and $E_{R(\cdot,\cdot)}(\cdot)$, where $R \leftarrow_{\$} \mathsf{Func}([u]\times\mathcal{M}_F,\mathcal{K}_E)$. Consequently, D' will simply be the distinguisher that runs D and answers its queries by applying E (keyed with the answers given by its own oracle) and will output the same value as D. Moreover, an adversary cannot use more than $|\mathcal{M}_F|$ different tweaks for a single user, which means that D' will make at most $\min(q, u\cdot|\mathcal{M}_F|)$ queries to F.

There also exists a $(\tau, q, t'')-$adversary D'' against the $\pm$mPRP$-$security of E such that

$$\left| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_{F^*}) \,:\, \mathsf{D}^{\mathsf{TKS}[E,F^*]_{f(\cdot)}} = 1\right] - \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{Perm}([u] \times \mathcal{M}_F, \mathcal{M}_E) \,:\, \mathsf{D}^{\widetilde{P}} = 1\right] \right| \leq \mathbf{Adv}_E^{\pm\mathrm{mPRP}}(\mathsf{D}''), \quad (2)$$

where $t'' = t + O(q)$. This can be seen as follows. Let D'' be the following adversary against the $\pm$mPRP security of E. D'' runs D, answering D's queries using its own oracle and by mapping each (user,tweak) value to a different user, and outputs the same value as D. In that case, the number of users queried would be smaller than $\tau = \min(q, u \cdot |\mathcal{M}_F|)$. By definition, for each (user,tweak) pair (u_i, t), $F^*_{f(u_i)}(t)$ is a uniformly random secret value chosen at the beginning of the experiment (with the random draw of f): the answers of the $\mathsf{TKS}[E, F^*]_{f(\cdot)}$ oracle thus follow the same distribution as the answers of a $\pm$mPRP oracle for E. Moreover, D'' does at most q queries in time at most $t + O(q)$.

The result follows by combining Eqs (1) and (2). □

5 A security analysis of the XORP PRP-to-PRF conversion method in the multi-user setting

5.1 Statement of the Result and Presentation of the Proof Strategy

For the remaining of this section, let us fix a non-zero number of users u and three positive integers n, s, w such that $s \leq wn$ and a block cipher E with key space $\mathcal{K}_E$ and message space $\{0,1\}^n$. We are going to study the mPRF security of the $\mathsf{XORP}_E^{w,s}$ construction and prove the following result.

Lemma 1 *Let q, t be integers such that $q \leq \frac{2^n}{67w^2(w+1)}$ and let D be a $(u, q, t)-$adversary against the* mPRF *security of $\mathsf{XORP}_E^{w,s}$. There exists a $(u, (w+1)q, t')-$adversary against the* mPRP *security of E such that*

$$\mathbf{Adv}^{\mathrm{mPRF}}_{\mathsf{XORP}_E^{w,s}}(\mathsf{D}) \leq \mathbf{Adv}^{\mathrm{mPRP}}_E(\mathsf{D}') + \frac{w^2 q}{2^n},$$

where $t' = O(t + q \cdot t_{XORP_{w,s}})$ and $t_{XORP_{w,s}}$ is an upper bound on the time needed to evaluate the $\mathsf{XORP}^{w,s}_{\cdot}$ construction.

Remark 4 This result is a slight generalization to the multi-user setting of a theorem from [21].

The remaining of the section is devoted to the proof of lemma 1. Let us denote E^* the perfect block cipher, i.e. the block cipher with key space $\mathcal{K}_{E^*} = \mathsf{Perm}(n)$, where

$$\forall (k, x) \in \mathcal{K}_{E^*} \times \{0,1\}^n,\ E^*_k(x) = k(x).$$

Let q, t be integers such that $q \leq 2^n/67w^2(w+1)$. We denote $n' = n - \lceil \log_2(w+1) \rceil$. Let D be a $(u, q, t)-$adversary against the mPRF security of the $\mathsf{XORP}^{w,s}_E$ construction. As usual, the first step of our proof is classical: we are going to replace the block cipher E in the construction by the perfect block cipher E^*. By definition, one has

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{mPRF}}_{\mathsf{XORP}^{w,s}_E}(\mathsf{D}) = & \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_E) \,:\, \mathsf{D}^{\mathsf{XORP}^{w,s}_E(f(\cdot),\cdot)} = 1\right] \\
& - \Pr\left[R \leftarrow_{\$} \mathsf{Func}([u] \times \{0,1\}^{n'}, \{0,1\}^s) \,:\, D^R = 1\right] \Big| \\
\leq & \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_E) \,:\, \mathsf{D}^{\mathsf{XORP}^{w,s}_E(f(\cdot),\cdot)} = 1\right] \\
& - \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_{E^*}) \,:\, \mathsf{D}^{\mathsf{XORP}^{w,s}_{E^*}(f(\cdot),\cdot)} = 1\right] \Big| \\
& + \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_{E^*}) \,:\, \mathsf{D}^{\mathsf{XORP}^{w,s}_{E^*}(f(\cdot),\cdot)} = 1\right] \\
& - \Pr\left[R \leftarrow_{\$} \mathsf{Func}([u] \times \{0,1\}^{n'}, \{0,1\}^s) \,:\, D^R = 1\right] \Big| \\
\leq & \mathbf{Adv}^{\mathrm{mPRP}}_E(\mathsf{D}') + \mathbf{Adv}^{\mathrm{mPRF}}_{\mathsf{XORP}^{w,s}_{E^*}}(\mathsf{D}), \qquad (3)
\end{aligned}$$

where D' is a $(u, (w+1)q, t')-$adversary D' against the mPRP security of E such that $t' = O(t + q \cdot t_{\mathrm{XORP}_{w,s}})$ and $t_{\mathrm{XORP}_{w,s}}$ is an upper bound on the time needed to evaluate the $\mathsf{XORP}^{w,s}_{\cdot}$ construction. Indeed, when f is uniformly random in $\mathsf{Func}([u], \mathcal{K}_{E^*})$, $E^*_{f(\cdot)}$ is a uniformly random multi-user permutation in $\mathsf{Perm}([u], n)$. Thus it is easy to see that

$$\begin{aligned}
& \Big| \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_E) \,:\, \mathsf{D}^{\mathsf{XORP}^{w,s}_E(f(\cdot),\cdot)} = 1\right] \\
& \quad - \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathcal{K}_{E^*}) \,:\, \mathsf{D}^{\mathsf{XORP}^{w,s}_{E^*}(f(\cdot),\cdot)} = 1\right] \Big| = \mathbf{Adv}^{\mathrm{mPRP}}_E(\mathsf{D}'),
\end{aligned}$$

where D' is the adversary against the mPRP security of E that simply runs D, outpuuts the same bit as D and answers D's queries by using its own oracle and by evaluating the XORP construction on the outputs.

We are now going to use the $H-$coefficients technique to prove that

$$\mathbf{Adv}^{\mathrm{mPRF}}_{\mathsf{XORP}^{w,s}_{E^*}}(\mathsf{D}) \leq \frac{w^2 q}{2^n}.$$

As this is now a purely information-theoretical problem, we are going to assume that D is computationally unbounded, and hence *wlog* deterministic.

5.2 The H-coefficients technique.

We start by describing Patarin's H-coefficients technique [38].

We summarize the interaction of D with its oracle in what is referred to as the *queries transcript* τ of the attack. We are also going to provide more information to the adversary. For each query, we are going to reveal the full output of the XORP construction (i.e. before the truncation) in the real world, and in the ideal world we will simply give him an equivalent number of random bits. This can only improve the distinguisher's advantage as this additional information can simply be ignored. More precisely, τ contains all triples $(i, x, y) \in [u] \times \{0,1\}^n \times \{0,1\}^{wn}$ such that D made the direct query (i, x) to the oracle and received answer y. Note that queries are recorded in an unordered fashion. However, since the distinguisher is assumed to be deterministic, there is a one-to-one mapping between this representation and the raw transcript of the interaction of D with its oracle (see e.g. [8] for more details). We also assume that D never makes useless queries and always makes the maximal number of queries, thus $|\tau| = q$.

We say that a queries transcript is *attainable*[5] if there exists an oracle F such that the interaction of D with F yields this transcript. Let us denote Θ the set of attainable transcripts. In all the following, we denote X_{re}, resp. X_{id}, the probability distribution of the transcript τ induced by the real world (resp. by the ideal world). By extension, we use the same notation to denote a random variable distributed according to each distribution. The main lemma of the $H-$coefficients technique is the following one.

Lemma 2 ([38, 8]) *Fix a distinguisher* D*. Let* $\Theta = \Theta_{\mathrm{good}} \sqcup \Theta_{\mathrm{bad}}$ *be a partition of the set of attainable transcripts. Assume that there exists* $\varepsilon_1 \geq 0$ *such that for any* $\tau \in \Theta_{\mathrm{good}}$*, one has*

$$\frac{\Pr[X_{\mathrm{re}} = \tau]}{\Pr[X_{\mathrm{id}} = \tau]} \geq 1 - \varepsilon_1,$$

and that there exists ε_2 *such that*

$$\Pr[X_{\mathrm{id}} \in \Theta_{\mathrm{bad}}] \leq \varepsilon_2.$$

Then $\mathbf{Adv}(\mathsf{D}) \leq \varepsilon_1 + \varepsilon_2$.

5.3 Preliminary observations.

Let us fix an attainable transcript

$$\tau = \{(u_1, x_1, y_1), \ldots, (u_q, x_q, y_q)\}.$$

For any message $x \in \{0,1\}^{wn}$ and for any $i \in \{1, \ldots, w\}$, $[x]_i$ will be the unique n-bit message such that $x = ||_{i=1}^{w} [x]_i$.

[5] That is with respect to D.

In the ideal world, the oracle is a uniformly random multi-user function, so that the probability of getting the attainable transcript τ is simply

$$\Pr\left[X_{\mathrm{id}} = \tau\right] = \frac{1}{2^{qwn}}.$$

In the real world, we want to evaluate the probability that a uniformly random function $f \in \mathsf{Func}([u], \mathsf{Perm}(n))$ satisfies, for $i = 1, \ldots, q$ and $j = 1, \ldots, w$,

$$f(u_i)(x_i||0) \oplus f(u_i)(x_i||j) = [y_i]_j.$$

In this case, we say that f is *compatible* with τ and this event will be denoted $f \in \mathsf{Comp}(\tau)$. Let m be the number of pairwise distinct users appearing in τ. For $i = 1, \ldots, r$, let τ_i be the transcript of the interaction of D with permutation $f(u_i)$, for an arbitrary ordering of the users, and let $q_i = |\tau_i|$. Then, one has $q = \sum_{i=1}^{r} q_i$ and $\tau = \bigcup_{i=1}^{r} \tau_i$. Since f is uniformly random in $\mathsf{Func}([u], \mathsf{Perm}(n))$, then the permutations $f(u_i)$ are uniformly random and independent in $\mathsf{Perm}(n)$. Then, the event $f \in \mathsf{Comp}(\tau)$ can be divided into r independent events $f(u_i) \in \mathsf{Comp}(\tau_i)$ for $i = 1, \ldots, r$. Thus, one has

$$\begin{aligned}
\Pr\left[X_{\mathrm{re}} = \tau\right] &= \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathsf{Perm}(n)) \,:\, f \in \mathsf{Comp}(\tau)\right] \\
&= \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathsf{Perm}(n)) \,:\, \bigcap_{i=1}^{r} f(u_i) \in \mathsf{Comp}(\tau_i)\right] \\
&= \prod_{i=1}^{r} \Pr\left[f \leftarrow_{\$} \mathsf{Func}([u], \mathsf{Perm}(n)) \,:\, f(u_i) \in \mathsf{Comp}(\tau_i)\right] \\
&= \prod_{i=1}^{r} \Pr\left[P \leftarrow_{\$} \mathsf{Perm}(n) \,:\, P \in \mathsf{Comp}(\tau_i)\right]. \qquad (4)
\end{aligned}$$

Let $i \in \{1 \ldots, r\}$. We are now going to evaluate the probability that a uniformly random permutation is compatible with $\tau_i = \{(u_i, x_1, y_1), \ldots, (u_i, x_{q_i}, y_{q_i})\}$. Let $\mathbf{y}_i = (y_1, \ldots, y_{q_i})$. For any permutation $P \in \mathsf{Perm}(n)$, let us denote $P(\tau)$ the $(w+1)q_i-$tuple defined as follows:

$$P(\tau) = \left(P(x_1|0), \ldots, P(x_1|w), \ldots, P(x_{q_i}|0) \ldots, P(x_{q_i}|w)\right).$$

We also denote by $\Lambda_w(\mathbf{y}_i)$ the set of every $(w+1)q-$tuple

$$P = (P_0, \ldots, P_{(w+1)q_i - 1}) \in J_n^{(w+1)q}$$

such that

$$\begin{cases}
P_0 \oplus P_1 = [y_1]_1 \\
\vdots \\
P_0 \oplus P_w = [y_1]_w \\
\vdots \\
P_{(w+1)(q_i-1)} \oplus \ldots \oplus P_{(w+1)q_i - w} = [y_{q_i}]_1 \\
\vdots \\
P_{(w+1)(q_i-1)} \oplus \ldots \oplus P_{(w+1)q_i - 1} = [y_{q_i}]_w.
\end{cases} \qquad (5)$$

Note that the event $P \in \mathsf{Comp}(\tau_i)$ is equivalent to $P(\tau) \in \Lambda_w(\mathbf{y})$. Thus, one has

$$\begin{aligned}\Pr\left[P \leftarrow_{\$} \mathsf{Perm}(n) \,:\, P \in \mathsf{Comp}(\tau_i)\right] &= \Pr\left[P \leftarrow_{\$} \mathsf{Perm}(n) \,:\, P(\tau) \in \Lambda_w(\mathbf{y})\right] \\ &= \sum_{\mathbf{P} \in \Lambda_w(\mathbf{y}_i)} \Pr\left[P \leftarrow_{\$} \mathsf{Perm}(n) \,:\, P(\tau) = \mathbf{P}\right] \\ &= \frac{|\Lambda_w(\mathbf{y}_i)|}{(2^n)_{(w+1)q_i}}. \end{aligned} \tag{6}$$

Combining Eqs (4) and (6), one gets

$$\Pr\left[X_{\mathrm{re}} = \tau\right] = \prod_{i=1}^{r} \frac{|\Lambda_w(\mathbf{y}_i)|}{(2^n)_{(w+1)q_i}}.$$

Finally, one has

$$p(\tau) := \frac{\Pr\left[X_{\mathrm{re}} = \tau\right]}{\Pr\left[X_{\mathrm{id}} = \tau\right]} = \prod_{i=1}^{r} \frac{2^{nwq_i}|\Lambda_w(\mathbf{y}_i)|}{(2^n)_{(w+1)q_i}}. \tag{7}$$

Hence, to apply lemma 2, like in the single-user case, we are going to need to compare, as precisely as possible, the quantities $|\Lambda_w(\mathbf{y}_i)|$ and $(2^n)_{(w+1)q_i}/2^{nwq_i}$.

In order to prove our result, we are going to rely on a combinatorial result by Patarin, who has already studied a related construction in the single-user setting in [39], and proven useful results in the context of the so-called Mirror Theory.

5.4 An Introduction to Mirror Theory

Introduced by Patarin (see e.g. [37,41]), Mirror Theory refers to the analysis of the number of solutions of systems of linear equalities and linear non-equalities in finite groups. This analysis is closely related to the security of various cryptographic constructions in the information theoretic model.

In this section, we are going to introduce the terminology of Mirror Theory and state Patarin's "Theorem $P_i \oplus P_j$ with any $\xi_{\max}$" [40], which is at the core of our proof of Lemma 1.

Definition 1 ([40]) Let (A) be a set of linear equations $P_i \oplus P_j = \lambda_k$, where $P_i, P_j \in \{0,1\}^n$. If, by linear combination of the equations in (A), we cannot generate an equation in only the λ_k variables, we will say that (A) has no *circle* in P, or that the equations of (A) are *linearly independent* in P.

In such a system of linear equations, some variables will be related by the fact that fixing the value of one such variable may in turn force the value of another one. This is formalized in the notion of block.

Definition 2 ([40]) We will say that two indices i and j are *in the same block* if we can obtain an equation only involving P_i, P_j and λ_k variables by linear combination of the equations in (A).

Definition 3 ([40]) We will denote by $\xi_{\max}$ the maximum nomber of indices that are in the same block.

With these definitions, we can now state Patarin's "Theorem $P_i \oplus P_j$ with any $\xi_{\max}$".

Theorem 3 ([40]) *Let (A) be a set of equations $P_i \oplus P_j = \lambda_k$ with α variables such that:*

1. *We have no circle in P in the equations (A).*
2. *We have no more than $\xi_{\max}$ indices in the same block.*
3. *By linearity from (A) we cannot generate an equation $P_i = P_j$ with $i \neq j$.*

Then, if $(\xi_{\max} - 1)^2 \alpha \leq \frac{2^n}{67}$, we have

$$2^{an} h_\alpha(A) \geq (2^n)_\alpha$$

where $h_\alpha(A)$ denotes the number of solutions of (A) that are also pairwise distinct and a is the number of equations in (A).

With this theorem, we can now proceed with the proof of Lemma 1.

5.5 Proof of Lemma 1.

First, let us define the set Θ_{bad} of bad transcripts. A transcript

$$\tau = \{(u_1, x_1, y_1), \ldots, (u_q, x_q, y_q)\}$$

is said *bad* if one of these two conditions is fulfilled.

1. There exists $i \in \{1 \ldots, q\}$, $j \in \{1, \ldots, w\}$ such that $[y_i]_j = 0$.
2. There exists $i \in \{1, \ldots, q\}$, $j, j' \in \{1, \ldots, w\}$ such that $j \neq j'$ and $[y_i]_j = [y_i]'_j$.

Note that these two conditions are required in order to satisfy condition 3. from Theorem 3. We are now going to upper bound the probability to get a bad transcript in the ideal world. In the ideal world, the distinguisher is simply interacting with a uniformly random function. Thus, one has

$$\Pr\left[X_{\text{id}} \in \Theta_{\text{bad}}\right] \leq \frac{wq}{2^n} + \frac{w(w-1)q}{2^n} = \frac{w^2 q}{2^n}. \tag{8}$$

We now have to lower bound the ratio $p(\tau)$. Recall that one has

$$p(\tau) := \prod_{i=1}^{r} \frac{2^{nwq_i} |\Lambda_w(\mathbf{y}_i)|}{(2^n)_{(w+1)q_i}}.$$

Each single-user transcript τ_i translates to a Mirror system (A_i) similar to Eqs (5). In order to lower bound the number of solutions to each system (i.e. $|\Lambda_w(\mathbf{y}_i)|$), we will rely on Theorem 3. Note that, in our case, each query translates to exactly one block of w equations and $w+1$ variables. Hence, for each system, we have $\xi_{\max} = w+1$, $a = wq_i$ and $\alpha = (w+1)q_i$.

The condition $(\xi_{\max}-1)^2\alpha \leq \frac{2^n}{67}$ from Theorem 3 becomes $w^2(w+1)q_i \leq \frac{2^n}{67}$ for $i = 1\ldots, m$, which is satisfied since $w^2(w+1)q \leq \frac{2^n}{67}$.

Moreover, if we look closely at system (5), we see that there can be no circle in P (i.e. it is not possible using the equations to generate by linearity an equation involving no P_i variable). Moreover, since τ is a good transcript, we see that it is impossible to generate an equation of the type $P_i = P_j$. As one has $|\Lambda_w(\mathbf{y}_i)| = h_{(w+1)q_i}(A_i)$, Theorem 3 gives

$$\begin{aligned} p(\tau) =& \prod_{i=1}^{r} \frac{2^{nwq_i}|\Lambda_w(\mathbf{y}_i)|}{(2^n)_{(w+1)q_i}} \\ =& \prod_{i=1}^{r} \frac{2^{nwq_i}h_{(w+1)q_i}(A_i)}{(2^n)_{(w+1)q_i}} \\ \geq& 1. \end{aligned} \tag{9}$$

Finally, if we combine Lemma 2 and Eqs (8) and (9), we get

$$\mathbf{Adv}^{\mathrm{mPRF}}_{\mathsf{XORP}^{w,s}_{E^*}}(\mathsf{D}) \leq \frac{w^2 q}{2^n},$$

which ends the proof of Lemma 1.

Acknowledgement This work has been supported in part by the European Union's H2020 Programme under grant agreement number ICT-644209. We would also like to thank the reviewers from Designs, Codes and Cryptography for their helpful comments.

References

1. Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Elmar Tischhauser, and Kan Yasuda. Parallelizable and Authenticated Online Ciphers. In Kazue Sako and Palash Sarkar, editors, *Advances in Cryptology - ASIACRYPT 2013 (Proceedings, Part I)*, volume 8269 of *LNCS*, pages 424–443. Springer, 2013.
2. Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. *Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements*, pages 259–274. Springer Berlin Heidelberg, Berlin, Heidelberg, 2000.
3. Mihir Bellare and Philip Rogaway. Introduction to modern cryptography, pseudorandom functions, 2005. http://cseweb.ucsd.edu/~mihir/cse207/classnotes.html.
4. Srimanta Bhattacharya and Mridul Nandi. Full indifferentiable security of the xor of two or more random permutations using the chi-squared method. In *Advances in Cryptology – EUROCRYPT 2018: 37th Annual International Cryptology Conference, Tel-Aviv, Israel*, Cham, 2018. Springer International Publishing. To appear.
5. Srimanta Bhattacharya and Mridul Nandi. A note on the chi-square method: A tool for proving cryptographic security. *Cryptography and Communications*, Jan 2018.

6. Eli Biham. How to decrypt or even substitute des-encrypted messages in 228 steps. *Inf. Process. Lett.*, 84(3):117–124, November 2002.
7. Debrup Chakraborty and Palash Sarkar. A General Construction of Tweakable Block Ciphers and Different Modes of Operations. In Helger Lipmaa, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology - Inscrypt 2006*, volume 4318 of *LNCS*, pages 88–102. Springer, 2006.
8. Shan Chen and John Steinberger. Tight Security Bounds for Key-Alternating Ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014. Full version available at http://eprint.iacr.org/2013/222.
9. Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking Even-Mansour Ciphers. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015 (Proceedings, Part I)*, volume 9215 of *LNCS*, pages 189–208. Springer, 2015. Full version available at http://eprint.iacr.org/2015/539.
10. Benoît Cogliati and Yannick Seurin. Beyond-birthday-bound security for tweakable even-mansour ciphers with linear tweak and key mixing. In *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 134–158. Springer, 2015.
11. Benoît Cogliati and Yannick Seurin. On the Provable Security of the Iterated Even-Mansour Cipher against Related-Key and Chosen-Key Attacks. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - Proceedings, Part I*, volume 9056 of *LNCS*, pages 584–613. Springer, 2015. Full version available at http://eprint.iacr.org/2015/069.
12. Paul Crowley. Mercy: A Fast Large Block Cipher for Disk Sector Encryption. In Bruce Schneier, editor, *Fast Software Encryption - FSE 2000*, volume 1978 of *LNCS*, pages 49–63. Springer, 2000.
13. Wei Dai, Viet Tung Hoang, and Stefano Tessaro. Information-theoretic indistinguishability via the chi-squared method. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology – CRYPTO 2017*, pages 497–523, Cham, 2017. Springer International Publishing.
14. Shimon Even and Yishay Mansour. A Construction of a Cipher from a Single Pseudorandom Permutation. *J. Cryptology*, 10(3):151–162, 1997.
15. Niels Ferguson, Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. The Skein Hash Function Family. SHA3 Submission to NIST (Round 3), 2010.
16. David Goldenberg, Susan Hohenberger, Moses Liskov, Elizabeth Crump Schwartz, and Hakan Seyalioglu. On Tweaking Luby-Rackoff Blockciphers. In Kaoru Kurosawa, editor, *Advances in Cryptology - ASIACRYPT 2007*, volume 4833 of *LNCS*, pages 342–356. Springer, 2007.
17. Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves. Improved masking for tweakable blockciphers with applications to authenticated encryption. In *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, pages 263–293, 2016.
18. Shai Halevi and Phillip Rogaway. A Tweakable Enciphering Mode. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, 2003.
19. Shai Halevi and Phillip Rogaway. A Parallelizable Enciphering Mode. In Tatsuaki Okamoto, editor, *Topics in Cryptology - CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, 2004.
20. Viet Tung Hoang and Stefano Tessaro. Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 (Proceedings, Part I)*, volume 9814 of *LNCS*, pages 3–32. Springer, 2016.
21. Tetsu Iwata, Bart Mennink, and Damian Vizár. Cenc is optimally secure. *IACR Cryptology ePrint Archive*, 2016:1087, 2016.

22. Jérémy Jean, Ivica Nikolic, and Thomas Peyrin. Tweaks and Keys for Block Ciphers: The TWEAKEY Framework. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 (Proceedings, Part II)*, volume 8874 of *LNCS*, pages 274–288. Springer, 2014.
23. K. Kurosawa. Power of a public random permutation and its application to authenticated encryption. *IEEE Transactions on Information Theory*, 56(10):5366–5374, Oct 2010.
24. Rodolphe Lampe and Yannick Seurin. Security Analysis of Key-Alternating Feistel Ciphers. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - FSE 2014*, volume 8540 of *LNCS*, pages 243–264. Springer, 2014.
25. Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable Blockciphers with Beyond Birthday-Bound Security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012*, volume 7417 of *LNCS*, pages 14–30. Springer, 2012. Full version available at http://eprint.iacr.org/2012/450.
26. Jooyoung Lee, Atul Luykx, Bart Mennink, and Kazuhiko Minematsu. Connecting tweakable and multi-key blockcipher security. *Designs, Codes and Cryptography*, Mar 2017.
27. Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable Block Ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002*, volume 2442 of *LNCS*, pages 31–46. Springer, 2002.
28. Atul Luykx, Bart Mennink, and Kenneth G. Paterson. Analyzing multi-key security degradation. Cryptology ePrint Archive, Report 2017/435, 2017. https://eprint.iacr.org/2017/435.
29. Bart Mennink. Optimally Secure Tweakable Blockciphers. In Gregor Leander, editor, *Fast Software Encryption - FSE 2015*, volume 9054 of *LNCS*, pages 428–448. Springer, 2015. Full version available at http://eprint.iacr.org/2015/363.
30. Bart Mennink. XPX: Generalized tweakable even-mansour with improved security guarantees. In *Advances in Cryptology - CRYPTO 2016 - Proceedings*, LNCS. Springer, 2016. To appear.
31. Bart Mennink. *Insuperability of the Standard Versus Ideal Model Gap for Tweakable Blockcipher Security*, pages 708–732. Springer International Publishing, Cham, 2017.
32. Kazuhiko Minematsu. Improved Security Analysis of XEX and LRW Modes. In Eli Biham and Amr M. Youssef, editors, *Selected Areas in Cryptography - SAC 2006*, volume 4356 of *LNCS*, pages 96–113. Springer, 2006.
33. Kazuhiko Minematsu. Beyond-Birthday-Bound Security Based on Tweakable Block Cipher. In Orr Dunkelman, editor, *Fast Software Encryption - FSE 2009*, volume 5665 of *LNCS*, pages 308–326. Springer, 2009.
34. Atsushi Mitsuda and Tetsu Iwata. Tweakable Pseudorandom Permutation from Generalized Feistel Structure. In Joonsang Baek, Feng Bao, Kefei Chen, and Xuejia Lai, editors, *ProvSec 2008*, volume 5324 of *LNCS*, pages 22–37. Springer, 2008.
35. Nicky Mouha and Atul Luykx. *Multi-key Security: The Even-Mansour Construction Revisited*, pages 209–223. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
36. Yusuke Naito. Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. *IACR Transactions on Symmetric Cryptology*, 2017(2):1–26, 2017.
37. Jacques Patarin. A Proof of Security in $O(2^n)$ for the Xor of Two Random Permutations. In Reihaneh Safavi-Naini, editor, *Information Theoretic Security - ICITS 2008*, volume 5155 of *LNCS*, pages 232–248. Springer, 2008. Full version available at http://eprint.iacr.org/2008/010.
38. Jacques Patarin. The "Coefficients H" Technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography - SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, 2008.
39. Jacques Patarin. Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. *IACR Cryptology ePrint Archive*, 2010:287, 2010.
40. Jacques Patarin. Security of balanced and unbalanced Feistel Schemes with Linear Non Equalities. 2010. Available at http://eprint.iacr.org/2010/293.
41. Jacques Patarin and Audrey Montreuil. Benes and butterfly schemes revisited. In *Proceedings of the 8th International Conference on Information Security and Cryptology*, ICISC'05, pages 92–116, Berlin, Heidelberg, 2006. Springer-Verlag.

42. Gordon Procter. A Note on the CLRW2 Tweakable Block Cipher Construction. IACR Cryptology ePrint Archive, Report 2014/111, 2014. Available at http://eprint.iacr.org/2014/111.
43. Phillip Rogaway. Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 16–31. Springer, 2004.
44. Phillip Rogaway, Mihir Bellare, and John Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Trans. Inf. Syst. Secur.*, 6(3):365–403, 2003.
45. Phillip Rogaway and Haibin Zhang. Online Ciphers from Tweakable Blockciphers. In Aggelos Kiayias, editor, *Topics in Cryptology - CT-RSA 2011*, volume 6558 of *LNCS*, pages 237–249. Springer, 2011.
46. Yu Sasaki, Yosuke Todo, Kazumaro Aoki, Yusuke Naito, Takeshi Sugawara, Yumiko Murakami, Mitsuru Matsui, and Shoichi Hirose. Minalpher v1. Submission to the CAESAR competition, 2014.
47. Richard Schroeppel. The Hasty Pudding Cipher. AES submission to NIST, 1998.
48. Stefano Tessaro. *Optimally Secure Block Ciphers from Ideal Primitives*, pages 437–462. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.
49. Lei Wang, Jian Guo, Guoyan Zhang, Jingyuan Zhao, and Dawu Gu. *How to Build Fully Secure Tweakable Blockciphers from Classical Blockciphers*, pages 455–483. Springer Berlin Heidelberg, Berlin, Heidelberg, 2016.